Multilevel Network Security Monitoring and Evaluation Model

Jin Yang
Department of Computer Science/LeShan Normal Univ., LeShan, China
Email:jinnyang@163.com

Tang Liu
College of Fundamental Education/Sichuan Normal Univ., Chengdu, China
Email: 253960818@qq.com

Lingxi Peng *
Department of Computer and Education software/Guangzhou Univ., Guangzhou, China
Email: bigluckboy@163.com

XueJun Li, Gang Luo
Department of Computer Science/LeShan Normal Univ., LeShan, China
Email:279718518@qq.com

***Abstract*—Based on the correspondence between the artificial immune system antibody and pathogen invasion intensity, this paper is to establish a real-time network risk evaluation model. According to the network intrusion own characteristics and the consequence from service, assets and attack, this paper design to build a hierarchical, quantitative measurement indicator system, and an unified evaluation information base and knowledge base. The paper also combines assets evaluation system and network integration evaluation system, considering from the application layer, the host layer, network layer may be factors that affect the network risks. The experimental results show that the new model improves the ability of intrusion detection and prevention than that of the traditional passive intrusion prevention systems.**

***Index Terms*—network security; artificial immune; intrusion detection**

I. INTRODUCTION

The traditional network security approaches include virus detection, frangibility evaluation, and firewall etc, e.g., the Intrusion Detection System (IDS) [1]. They rely upon collecting and analyzing the viruses' specimens or intrusion signatures with some traditional techniques [2]. Moreover, being lack of self-learning and self-adapting abilities, they can only prevent those known network intrusions, and can do nothing for those variety intrusions. Recent years, the artificial immune system has the features of dynamic, self-adaptation and diversity [3-6] that just meet the constraints derived from the characteristics of the grid environment, and mobile agent has many same appealing properties as that of artificial immune system. Negative Selection Algorithm and the concept of computer immunity proposed by Forrest in 1994 [7-8]. In contrast, the AIS theory adaptively generates new immune cells so that it is able to detect previously unknown and rapidly evolving harmful antigens [9]. However, much theoretical groundwork in immunological computation has been taken up, but there is a lack of perfectly systems based AIS of dynamical immunological surveillance for network security.

Based on the correspondence between the artificial immune system antibody in the artificial immune systems and pathogen invasion intensity, this paper is to establish a network risk evaluation model. According to the network intrusion own characteristics and the consequence from service, assets and attack, we design to built a hierarchical, quantitative measurement indicator system, and an unified evaluation information base and knowledge base. This model will help the network managers evaluate the possibility and the graveness degree of the network dangerous quickly, ease the pressure of recognition, to get targeted immediate defense strategy of the strength and risk level of the current network attacks.

II. THE EVALUATION OF THE NETWORK DANGER

The biological immune system can produce antibodies to resist pathogens through *B* cells distributing all over the human body. And *T* cells can regulate the antibody concentration. Simulating biological immune system, we place a certain amount of immune cells into the network, and perceive the surrounding environment. Simulating creatural immune system, we place a certain amount of

* Corresponding author.

This work is supported by the National Natural Science Foundation of China under Grant (No.61003310) and the Scientific Research Fund of Sichuan Provincial Education Department (No. 10ZB005).

doi:10.4304/jsw.6.5.806-813

immune cells into the network, and perceive the surrounding environment of the detectors. As soon as the immune detectors detect an attack, the detectors begin clone and generate a mass of similar detectors in order to defend from fiercer network attacks and warn the dangerous level of the network [10]. While the network danger become abating, the corresponding numbers of antibodies will decrease at the same time. The detectors' number and type reflect the attack's intensity and type suffered by the network intrusion. In this model, the detectors can be categorized, according to the evolvement progress of the detectors themselves, into 3 types, viz. immature detectors, mature detectors and memory detectors, and the content will be expatiated in detail in the following.

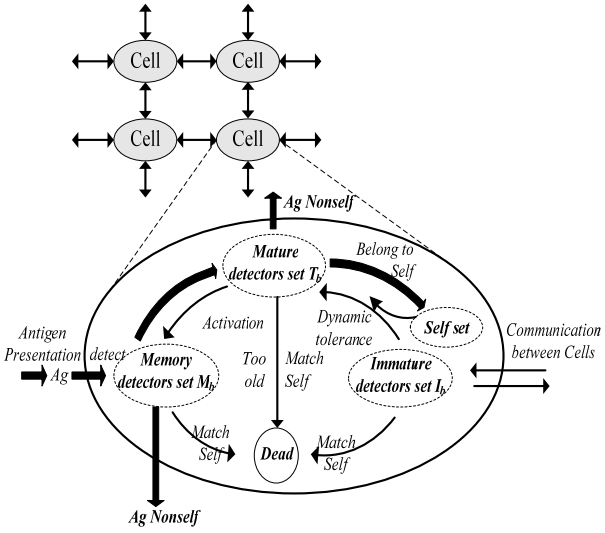

Figure 1. The Framework of danger-detecting in the NDEMAIS

III. THE DYNAMICAL IMMUNOLOGICAL SURVEILLANCE MODEL BASED ON AIS

A. The Definition of Antigen, Antibody, Self and Non-self

Definition: Antigens (Ag , $Ag \subset U$, $D = \{0,1\}^l$) are fixed-length binary strings extracted from the Internet Protocol (IP) packets transferred in the network. The antigen consists of the source and destination IP addresses, port number, protocol type, IP flags, IP overall packet length, TCP/UDP/ICMP fields [11-12], etc. The structure of an antibody is the same as that of an antigen. For virus detection, the nonself set (*Nonself*) represents IP packets from a computer network attack, while the self set (*Self*) is normal sanctioned network service transactions and nonmalicious background clutter. Set Ag contains two subsets, $Self \subseteq Ag$ and $Nonself \subseteq Ag$ such that

$$Self \cup Nonself = Ag \text{ and } Self \cap Nonself = \Phi . \quad (1)$$

B. The Dynamic Equations of the Mature Detectors

$$T_b = \{x \mid x \in B, \forall y \in Self \ \ (< x.d, y > \notin Match \wedge x.count < \beta)\} \quad (2)$$

$$T(t) = T(0) = 0, \ \ t = 0 \quad (3)$$

$$T(t+\Delta t) = T(t) + T_{new}(\Delta t) - T_{match\_self}(\Delta t) - T_{dead}(\Delta t) - T_{active}(\Delta t) \quad (4)$$

$$T.age(t+\Delta t) = T.age(t) + 1, \quad when \quad T.age(t+\Delta t) < \lambda \quad (5)$$

$$T_{match\_self}(t+\Delta t) = \frac{\partial T_{match\_self}}{\partial x_{match\_self}} T(t), \quad \text{when } f_{match}(T(t-1), Self(t-1)) = 1 \quad (6)$$

$$T.count(t+\Delta t) = T.count(t) + 1 \quad (7)$$

$$T_{active}(\Delta t) = \frac{\partial T_{active}}{\partial x_{active}} \cdot \Delta t, when \quad T.count(t+\Delta t) \geq \beta \quad (8)$$

$$T_{dead}(\Delta t) = \frac{\partial T_{death}}{\partial x_{death}} \cdot \Delta t, \quad \text{when} \quad T.count(t+\Delta t) < \beta, \text{and} T.count > \lambda \quad (9)$$

$$\frac{\partial T_{active}}{\partial x_{active}} \cdot \Delta t = I_{maturatiion}(t), T.\rho(\Delta t) = 0, \quad \text{when} \quad I.age(t) > \alpha \quad (10)$$

Equation (4) depicts the lifecycle of the mature detector, simulating the process that the mature detectors evolve into the next generation. All mature detectors have a fixed lifecycle (λ). If a mature detector matches enough antigens ($\geq \beta$) in its lifecycle, it will evolve to a memory detector. However, the detector will be eliminated and replaced by new generated mature detector if they do not match enough antigens in their lifecycle. $T_{new}(t)$ is the generation of new mature detector. $T_{dead}(t)$ is the set of detector that haven't match enough antigens ($\leq \beta$) in lifecycle or classified self antigens as *nonself* at time *t*. $T(t+\Delta t)$ simulates that the mature detector undergo one step of evolution. $T_{dead}(t)$ indicates that the mature detector are getting older. $T_{active}(t)$ is the set of the least recently used mature detector which degrade into Memory detector and be given a new age $T > 0$ and count $\beta > 1$. Because the degraded memory detector has better detection capability than mature detector, it is better to form a memory detector. When the same antigens arrive again, they will be detected immediately by the memory detector. In the mature detector lifecycle, the inefficient detectors on classifying antigens are killed through the process of clone selection. Therefore, the method can enhance detection efficiency when the abnormal network behaviors intrude the system again.

In the course, λ is the threshold of the affinity for the activated detectors. The affinity function $f_{match}(x, y)$ may be any kind of Hamming, Manhattan, Euclidean, and *r*-continuous matching, etc. In this model, we take *r*-continuous matching algorithm to compute the affinity of

mature detectors. The matching functions utilize the following definitions:

$$f_{\text{match}}(x,y)=\begin{cases}1 & \exists i,\ j,\ j-i\geq r\wedge 0<i<j\leq l,\\ & x_i=y_i, x_{i+1}=y_{i+1},\cdots,x_j=y_j\\ 0 & otherwise\end{cases} \tag{11}$$

The *r*-continuous matching is commonly used method for measuring the distance between bit strings with the goal of producing a better similarity coefficient.

C. The Dynamic Equation of Memory Detectors

$$M(t)=M(0)=0,\qquad t=0 \tag{12}$$

$$M(t+\Delta t)=M(t)+M_{new}(\Delta t)+M_{from\_other}(\Delta t)-M_{dead}(\Delta t),\quad when\quad f_{match}(M(t),Ag(t))\neq 1\quad,\quad t>1, \tag{13}$$

$$M(t+\Delta t)=M(t)+M_{clone}(t)+M_{new}(\Delta t)+M_{from\_other}(\Delta t)-M_{dead}(\Delta t), when\quad f_{match}(M(t),Ag(t))=1 \tag{14}$$

$$M_{clone}(t)=\frac{\partial M_{clone}}{\partial x_{clone}}\cdot\frac{\partial M_{active}}{\partial x_{active}}\cdot\Delta(t-1),\quad when\quad f_{match}(M(t),Ag(t))=1 \tag{15}$$

$$M_{clone}(t+\Delta t)=M_{clone}(t), M.\rho(t+\Delta t)=M.\rho(t)+V_p\cdot\Delta t,\quad M.count(t+\Delta t)=M.count(t)+1 \tag{16}$$

$$M.\rho(t+\Delta t)=\frac{1}{2}\cdot M.\rho(t), M.age(t+\Delta t)=M.age(t)+1,\quad when\quad f_{match}(M(t),Ag(t))\neq 1 \tag{17}$$

$$M_{new}(\Delta t)=\frac{\partial M_{new}}{\partial x_{new}}\cdot\Delta t=\frac{\partial T_{active}}{\partial x_{active}}\cdot\Delta(t-1)\ ,\ M_{new}\cdot\rho(t)=\rho_0 \tag{18}$$

$$M_{dead}(\Delta t)=\frac{\partial M_{death}}{\partial x_{death}}\cdot\Delta t, when\quad f_{match}(M(t-1),Self(t-1))=1 \tag{19}$$

$$M_{from\_other}(\Delta t)=\sum_{i=1}^{k}(\frac{\partial M^{i}_{from\_other}}{\partial x_{from\_other}}\cdot\Delta t) \tag{20}$$

Equation (13) depicts the dynamic evolution of memory detector. $M(t+\Delta t)$ simulates the process that the memory detector evolve into the next generation ones. $M_{new}(t)$ is the set of memory detector that are activated by antigens lately. These mature detector matched by an antigen will be activated immediately and turn to a memory detector. $M_{dead}(t)$ is the memory detector that be deleted if it matches a known self antigen. $M_{clone}(t)$ is the reproduced memory detector when the detector distinguish a antigens. $M_{from\_other}(t)$ is the memory detector that transformed from other computers. The *k* indicates that the *ID* number of the computer. Therefore, dynamic model of immune is to generate more antibodies and enhance the ability of self-adaptation for the system.

D. The Dynamic Model of Self

In a real-network environment some network services and activities are often change, which were permitted in the past but may be forbidden at the next time.

$$I(t)=I(0)=\{x_1,x_2,...,x_n\},\qquad t=0 \tag{21}$$

$$I(t+\Delta t)=I(t)+I_{new}(\Delta t)-I_{match\_self}(\Delta t)-I_{maturation}\cdot\Delta t \tag{22}$$

$$I.age(t+\Delta t)=I.age(t)+1 \tag{23}$$

$$I_{match\_self}(t+\Delta t)=I(t), when\quad f_{match}(I(t-1),Self(t-1))=1 \tag{24}$$

$$I_{maturatiio\,n}(t+\Delta t)=I(t),\qquad I.age(t+\Delta t)>\alpha \tag{25}$$

$$I_{new}(\Delta t)=(\xi_1\cdot\frac{\partial I_{\text{random}}}{\partial x})\cdot\Delta t+(\xi_2\cdot\frac{\partial I_{\text{inherit}}}{\partial x})\cdot\Delta t \tag{26}$$

Equation (22) stimulates the dynamic evolution of self-antigens, where $x_i\in\Re(i\geq 1, i\in N)$ is the initial self element defined. I_{new} is the set of newly defined elements at time *t*, and $I_{maturation}$ is the set of mutated elements. $f_{match}(y,x)$ is used to classify antigens as either self or nonself: if *x* is a self-antigen, return 0; if *x* is a nonself one, return 1; if *x* is detected as nonself but was detected as a self-antigen before, then it may be a nonself antigen (needs to be confirmed), and return 2. There are two advantages in this model. (1) *Self immune surveillance*: The model deletes mutated self-antigens ($I_{maturation}$) in time through surveillance. The false-negative error is reduced. (2) *The dynamic growth of Self*: The model can extend the depiction scope of self through adding new self-antigens (I_{new}) into *Self*. Therefore, the false-positive error is prevented.

E. The Antibody Cross

In order to keep the variety of individual as well as the optimal solution can be achieved, we divide the antibody gene to *n* gene bits set and utilize multi-point cross process. For example, we select two gene by random such as $G_1=\{g_1,g_2,\cdots,g_i,\cdots g_n\}$, $G_2=\{g_1^{'},g_2^{'},\cdots,g_i^{'},\cdots g_n^{'}\}$, Select some points randomly, and then form two-point pair with some probability (*p*) to cross operation, to generate cross point set, and then to generate new gap of set $G_{new}=\{g_1,g_2,\cdots,g_i^{'},\cdots g_n\}$. Select cross point according to binomial distribution

$$P\{X=k\}=\binom{n}{k}p^k(1-p)^{n-k}, k=0,1,2,\ldots,n\ .\ 0<p<1 \tag{27}$$

$E(X) = np$, $D(X) = np(1-p)$, where X is the numbers of cross points. Then the G_1 and G_2 turn into the offspring G_{new} by the cross process.

F. Antibody Variation

In order to prevent algorithm from converging prematurely, we take variation operation to the Gene set $G_1 = \{g_1, g_2, \cdots, g_i, \cdots g_n\}$ after the cross process. Select variation point randomly and varied with some variation probability (p_m) to generate new generation $G_{new} = \{g_1, g_2, \cdots, g_i^{'}, \cdots g_n\}$. Select variation point according to Poisson distribution

$$P\{X = k\} = \frac{\lambda^k e^{-\lambda}}{k!}, k = 0,1,2,\cdots \quad (28)$$

$E(X) = D(X) = \lambda > 0$, where X is the numbers of variation points. Then the G_1 turn into the offspring G_{new} by the variation process.

G. The Process of Immunological Surveillance

These response processes can be divided into two stages: primary immune response, secondary immune response. When the same antigen intrude into the body for the second time, because of the organism have some antibody to identify the antigen, the immune system can respond quickly and come into being a large number of homothetic antibodies in order to clear the rapid antigen in the body. The rapid process is known as secondary immune response.

Memory detectors M_b(t) express that the system has suffering various attacks at moment *t*. Memory detectors' concentration value of antibody is ρ(t). ρ(t) shows that at current time the system is suffering what kind of attacks and computes the intensity and categories. It is one of the important indicators of reflection the current system network intrusion danger level. There are two major changes probability of antibody concentration.

(1) The increase of the antibody concentration: When the memory detector antibody captures a particular antigen, representing have detecting a kind of invasion, we increase the antibody concentration. We use $V_\rho(t)$ reflects the rate of increase of antibody concentration. Therefore, at moment *t* the antibody concentration ρ(t) of M_b(t) is: $\rho(t)=\rho(t-1)+ V_\rho \cdot \Delta t$. Affected by the antigen, the more intensive invasion antigens, the faster at the increase rate of antibody concentration. Taking into account the emergence of the invasion was a random act, such as biodynamic body falling on the ground, such as trees fluttering in the wind, the random movement of the rate could be subject to Gaussian distribution. Antigen number *x* and the variety speed excitation function of antibody concentration $V_\rho(x)$ accord with the Gaussian distribution with parameters (h, μ), and these nonlinear causal relationship can be expressed as follows: (which, *x* is the number of memory detector detecting the invasion in period of time.)

$$V_\rho(x) = \frac{\mathrm{A}}{\sqrt{2\pi}\sigma} e^{-\frac{[(x-h)\cdot u]^2}{2}}, \quad u > 0, \quad 0 < x < +\infty \quad (29)$$

In order to avoid detection unlimited cloning, we regulate A is the largest concentration of limiting growth. Since the each invasion of antigen make different impact on the network and host, we define μ parameters to reflect the extent of the damage caused by antigens. The greater of μ value the faster of the antibody concentration increase speed, and also shows the more dangerous of the antigens captured by the antibody. Parameters h shows that the antigen stimulate the antibody to the limit when stimulation course achieve to a certain extent.

*(2) The attenuation of the antibody concentration***:** In organisms these antibodies which stimulated by some certain antigens will gradually disappear after a certain period of time. In our system, if the memory detector in the next step failed to clone once more, we set the antibody concentration turn into its attenuation phase, in accordance with the following.

$$\rho(t) = \frac{1}{2}\rho(t-\tau), \tau \le t \le T \quad (30)$$

After each half life τ, if the detector did not find any antigen, the antibody concentration will reduce by half. When the antibody concentration decay to ε_τ, it will stop decaying, showing that the act of invasion has disappeared. In the mature-detector lifecycle, the inefficient detectors on classifying antigens are killed through the process of clone selection. However, the efficient detectors on classifying antigens will evolve to memory detectors. Therefore, similar antigens representing abnormal network behaviors can be detected quickly when they intrude the system again as secondary immune response.

Ⅳ. THE EVALUATION OF THE NETWORK DANGER

After we describe the network attacking actions, it is necessary to evaluate the dangerous degree of the network, and judge the severity of the attacking actions. Network dangers are of diversity (because of many affecting factors) and of randomicity. Thus, evaluation is a process involving numerous complicated factors. The essence of evaluation is to hierarchically grade each evaluation factor in terms of its weight in order to ultimately reflect the dangerous degree of the entire network.

Our model simulates the process that metabolism and competition of the cells organism through the use of continuous renovation and enrichment process. The values of M_b reflect the intensity of intrusion in current network. Therefore, system evaluates the network security by perceiving the danger around of them. Owing to the fact that our model relates to enormous factors for evaluation, on purpose of reasonably and entirely

measuring the network dangerous status, we classify the involved factors as host dangers, area dangers, detectors dangers, and special dangers. The host dangers mainly arise out of the dangers which are possessed by each host computers; the area dangers are divided by regions; the detector dangers are those factors which determined in terms of antibody consistencies, antibody consistencies change speed, and detector types; and particular dangers refer to the second corresponding time and responding speed etc. Afterwards, we subdivide and arrange all the factors which influence the network dangers, in order to let them locate on different layers, forming a structure model with identify matrix. In the traditional evaluation system, the choice usually was made according to few of main factors, taking into account other factors merely as references, and then simply described the happening possibility of the dangers by high, medium and low. Hence, many factors which cannot be quantified were always ignored, so that the traditional system can not evaluate the varying situation where there are various factors and conditions involved at the same time, which more often than not give rise to the result that evaluation decisions are void of comprehensiveness and that the outcomes are distorted.

In our evaluation model we utilize the AHP (Analytic Hierarchy Process) Principle provided by operational research expert T. L. Saaty to evaluate the network dangerous situation. This method can efficiently cope with those complex problems which are difficult to be solved by quantitative methods. Its characteristics are: firstly, it can break complex questions down to some gradations, then analyze progressively on the layers much simpler than before in order to express and handle the decision-makers' subjective judgments through quantity format. Next, it calculates by mathematics the weight of the sequence of relative significance of the factors on each layer. Via the general permutation among all the layers, compute and rank the relative weight of all the factors. We synthetically consider the qualitative and quantitative factors during the evaluation process, adopt the AHP Principle, so as to provide reasonable methods and instruments for comprehensive evaluation of the network dangerous situation.

A. Computation the Hiberarchy of the Model

Owing to the fact that our model relates to enormous factors for evaluation, on purpose of reasonably and entirely measuring the network dangerous status, we classify the involved factors as host dangers, area dangers, cells dangers, and special dangers. The host dangers mainly arise out of the dangers which are possessed by each host computers; the area dangers are divided by regions; the cell dangers are those factors which determined in terms of cell consistencies, cell-varying speed, and cell types; and particular dangers refer to the second corresponding time and responding speed etc. Afterwards, we subdivide and arrange all the factors which influence the network dangers, in order to let them locate on different layers, forming a structure model with identify matrix. The following danger evaluation model is divided in to the general object layer (A), the standard layer (B), and the factor layer (C) (see Fig. 2). Furthermore, to get the weight values of these factors, this model adopts the AHP method. The underlying idea is to compare and estimate the eigenvalue λ_i of the special equation of the matrix B by way of seeking a solution, then find out the maximum eigenvalue $\lambda_{\max}$ and get its corresponding eigenvector $X=(x_1, x_2, \cdots, x_n)$. Finally, we will get relative weight vector $A=(w_1, w_2, \cdots, w_n)$ after merging all eigenvectors into one. In a word, the entire method can be approximately reduced to four steps, that is, ① establish hierarchical structure model; ② construct evaluation matrices; ③ calculate factors' relative weight under a coincident standard; ④ compute the integrated weight of the factors on each layer. Hereinafter, the evaluation process will be introduced in detail.

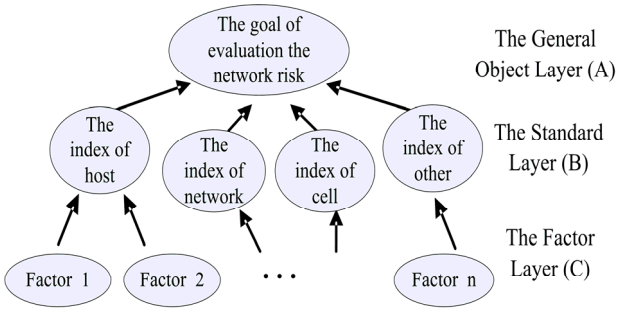

Figure 2. The hierarchy of network danger evaluation model

B. Computing Single Weight

1) Construct Identify Matrix: First of all, we must construct identify matrix which is result that we compared the relative importance of one group of elements on next layer with some past layer element constraint. That is, it shows the relative importance of any pair of factors. In detail, denote b_{ij} the compared result of the i^{th} factor and j^{th} one, b_{ij} all together form the identify matrix B:

$$B=\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$$

Where: $b_{ii}=1$ if $i=j$ and $b_{ij}=1/b_{ji}$ if $i\neq j$.

2) Computing Weights: Next we obtain the weight of each factor. According to the identify matrix B, we can get the maximum eigenvalue of the matrix $\lambda_{\max}$. Here, we can get the maximum $\lambda_{\max}$ according with the following contidion:

$$\begin{vmatrix} b_{11}-\lambda & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22}-\lambda & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1} & b_{n2} & \cdots & b_{nn}-\lambda \end{vmatrix}=0$$

Work out the corresponding eigenvector of maximum eigenvalue of B, $X=(x_1,x_3,\cdots,x_n)$, let x_i to be the weight of factor u_i, then we can get unitary weights denote W_i.

$$A=(W_1,W_2,\cdots,W_n)=(x_1/\sum_{i=1}^{n}x_i,x_2/\sum_{i=1}^{n}x_i,\cdots,x_n/\sum_{i=1}^{n}x_i,)$$

3) Test of Consistency: Because of complexity of evaluation and limit of individual knowledge, the individual identify matrix may not be consistent with the actual one, or the disagreement of any two identify matrixes may result in error of subjective judgment. However, we must test the consistency of the matrix B as follows:

① Computing consistency value $C\cdot I$

$$C\cdot I=\frac{\lambda_{\max}-n}{n-1} \tag{31}$$

② Computing consistency ratio $C\cdot R$

$$C\cdot R=\frac{C\cdot I}{R\cdot I} \tag{32}$$

Where $R\cdot I$ is mean consistency value that can be found in the reference and forms, we often consider that if $C\cdot R$ is smaller than 0.1, the consistency of matrix is acceptable, otherwise we must modify the identify matrix B.

4) Computing the General Weight Order: The general weight order means that the weight order comparing the elements in the present layer and the highest layer. We have got each order of element in rule layer to the object layer and the values are $W_1,W_2,\cdots,W_n$, respectively, we also know that order that design layer to the rule layer and the values are $W_1^j,W_2^j,\cdots,W_n^j$, then the general order is

$$V=W^jW=\begin{pmatrix}W_1^j & W_1^j & \cdots & W_1^j\\ W_2^j & W_2^j & \cdots & W_2^j\\ \vdots & \vdots & \vdots & \vdots\\ W_n^j & W_n^j & \cdots & W_n^j\end{pmatrix}\begin{pmatrix}W_1\\ W_2\\ \vdots\\ W_n\end{pmatrix}=\begin{pmatrix}V_1\\ V_2\\ \vdots\\ V_n\end{pmatrix}, \tag{33}$$

C. Evaluating the danger level

The entire network of danger level should fully reflect the value of each of the host facing attacks. As the host of each position is not the same such as running a different system for different users and providing different services, influencing different economic, affecting different social and even political values, they are in possession of different essentiality.

Let $n_{ij}(t)$ be the numbers of i^{th} computers detect attacking at time t. Let $\beta_i(0\le\beta_i\le1)$ be the importance coefficient of ith computer in the network and α_j $(0\le\alpha_j\le1)$ be the danger coefficient of the j^{th} kind of attack in the network. Then, we can define the attack intensity $r_i(t)$ of the j^{th} kind of attack and the corresponding network danger $r_i(t)$ as follows:

$$r_i(t)=\frac{2}{1+e^{-\sum_j\alpha_j n_{ij}}}-1 \tag{34}$$

Let $\text{Importance}_i=\sum_{k=1}^{8}(I_k\times W_k)$ be the importance coefficient of j^{th} host in the network. Then, we obtain the network entire danger level value: $R(t)$ =∑(indicator value × indicator weight). Therefore, we can get network danger $R(t)$ situation and evaluate network security at real time.

$$\begin{aligned}R(t)&=\tanh(\sum_{m=1}^{N}(\sum_{i=1}^{n}(Host_i\text{'s}\ \ danger\times\text{Importance}_j)\times LCRS\_Weight_m))\\&=\tanh(\sum_{m=1}^{N}(\sum_{i=1}^{n}(Host_i\text{'s}\ \ danger\times\sum_{k=1}^{8}(I_{j,\ k}\times W_k))\times LCRS\_Weight_m))\\&=\tanh(\sum_{m=1}^{N}(\sum_{i=1}^{n}(r_i(t)\times\sum_{k=1}^{8}(I_{j,\ k}\times W_k))\times LCRS\_Weight_m))\end{aligned} \tag{35}$$

The conclusion can be shown that the higher value $R(t)$ reaches the more dangerous the network is.

Ⅴ.EXPERIMENTAL RESULTS AND ANALYSIS

A. *Experimental Environment* and Evaluation Indicators

Experiments of attack simulation were also carried out in our Laboratory. Analytic Hierarchy Process is applied to our model to evaluate the weights of the indicators in the experiments. Considering the preciseness and efficiency, we use 12 indicators to evaluate the network danger, which include host danger, area danger, cells danger, special danger etc. The weights of the indicators are evaluated and sorted by orders and the mapping of all hierarchies can be seen in Table 1.

TABLE I
Weight Orders of All Layers

	B_1 0.0969	B_2 0.0485	B_3 0.8253	B_4 0.0293	W
C1	1				0.0969
C2		1			0.0485
$C3_1$			0.3801		0.3137
$C3_2$			0.4029		0.3325
$C3_3$			0.0934		0.0771
$C3_4$			0.1235		0.1020
$C4_1$				0.3333	0.0097
$C4_2$				0.6667	0.0195

Evaluate the above indicators: C.R = 0.036 < 0.1. It has a satisfactory consistency. Consequently, the weights of the indicators in the *NAIMAI* can be evaluated as the following: host dangers: 0.0969, area dangers: 0.0485, cells dangers: 0.8253, special dangers: 0.0293 and others dangers: 0.0969, 0.0485, 0.3137, 0.3325, 0.0771, 0.1020, 0.0097, and 0.0195. The conclusion can be draw that the higher values $R(t)$ reaches , the more dangerous the network is. Otherwise, the lower the $R(t)$ is, the safer the network is.

An antigen was defined as a fixed length binary string composed of the source/destination IP address, port number, protocol type, IP flags, IP overall packet length, TCP/UDP/ICMP fields, and etc. The network was attacked by 20 kinds of attacks, such as Syn Flood, Land, Smurf, and Teardrop. A total of 20 computers in a network were under surveillance. The task aimed to detect network attacks. Here are the coefficients for the model. We use *r-contiguous* bits matching rule (r=8) for computing the affinity, n=40 (the size of initial self set), and ξ =4 (the number of new generated immature detectors). The activation threshold is β ; tolerance period is λ .

B. Results and Analysis

Figure 3 illustrates the syn attacks. Figure 4 depicts the evaluation of the network danger in our model.

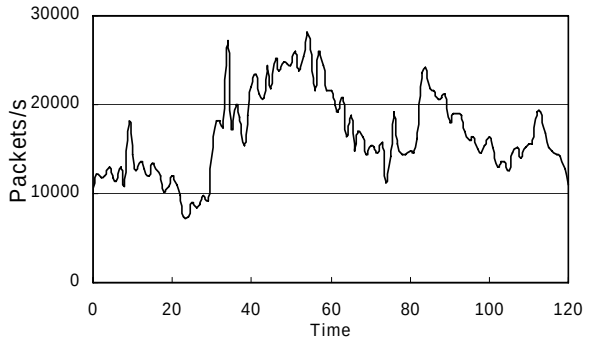

Figure 3. The network suffering from the syn incursions for instance

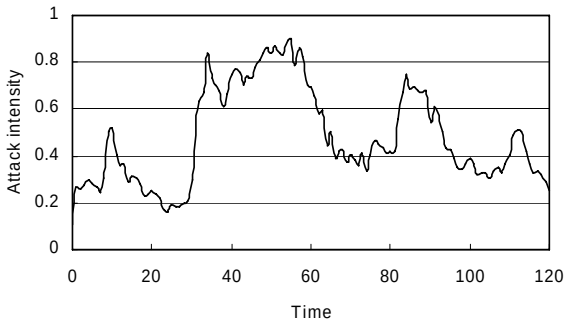

Figure 4. The line of the network dangers obtained by our model at these incursions

As is shown in Figure 4, $R(t)$ changes when attack levels changes. The rise in attack levels is accompanied by a corresponding increase in $R(t)$, as implies the bad network security. On the other hand, if attack levels decline, $R(t)$ decreases accordingly after seconds of delay. Therefore, the network can stays on guard even when the attacks occur once again during a very short time.

VI. CONCLUSIONS

This paper combines the risk evaluation methods with application security engineering principles, and can change current passive defense situation using traditional network security approaches, and is helpful to establish new generation proactive defense theories and realization techniques. At the same time, the work is of not only theoretic values to design proactive defense systems which have intrusion tolerant ability and survivability in any complex network circumstances, but also very significant to protect network infrastructure. The experimental results show that the proposed model has the features of real-time processing that provide a good solution for network surveillance.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China under Grant (No.61003310) and the Scientific Research Fund of Sichuan Provincial Education Department (No. 10ZB005).

REFERENCES

[1] Thomas, Ciza, Balakrishnan, N. Performance enhancement of Intrusion Detection Systems using advances in sensor fusion. Information Fusion, 2008 11th International Conference on June 30 , (2008):1-7

[2] Abdoul Karim Ganame, Julien Bourgeois, Renaud Bidou, Francois Spies. A global security architecture for intrusion detection on computer networks. Computers & Security, 27(1), 2008:30-47

[3] Vasilios Katos. Network intrusion detection: Evaluating cluster, discriminant, and logit analysis. Information Sciences, 177(15), (2007), 3060-3073.

[4] Agustín Orfila, Javier Carbó, Arturo Ribagorda. Autonomous decision on intrusion detection with trained BDI agents. Computer Communications, 31(9), (2008),1803-1813.

[5] Vincent Toubiana, Houda Labiod, Laurent Reynaud, Yvon Gourhant. A global security architecture for operated hybrid WLAN mesh networks. Computer Networks, 54(2),2010: 218-230

[6] Kuby J.: Immunology. Fifith Edition by Richard A. Goldsby et al.

[7] F.M.Burnet. The Clone Selection Theory of Acquired Immunity. Gambridge: Gambridge University Press (1959)

[8] S A Hofmeyr, and S Forrest. Architecture for an artificial immune system. Evolutionary Computation, vol. 8 (2000) 443-473

[9] S Forrest, A S Perelson, L Allen, and R Cherukuri. Self-Nonself Discrimination in a Computer. Proceedings of IEEE Symposium on Re-search in Security and Privacy, Oakland, (1994)

[10] Panigrahi BK, Yadav SR, Agrawal S, et al. A clonal algorithm to solve economic load dispatch. Electric Power Systems Research. 77(10), (2007):1381-1389

[11] Tao Li. An immune based dynamic intrusion detection model. Chinese Science Bulletin. 50, (2005): 2650-2657

[12] Tao Li. An immunity based network security risk estimation. Science in China Ser. F Information Sciences. 48 (2005):557- 578

Jin Yang received his M.S. degree and the Ph.D. degree in computer science from Sichuan University, Sichuan, China. He is an Associate Professor in Department of Computer Science at LeShan normal university. His main research interests include network security, artificial immune, knowledge discovery and expert systems.

Tang Liu received his M.S. degree in College of Computer Science, Sichuan University, China, in 2009. Since 2008, he has been a instructor in College of Fundamental Education, Sichuan Normal University. His research interests are in the area of wireless sensor networks.

Lingxi Peng born in 1978. Associate professor, Ph.D. and senior membership of China. His main research interests include network security and artificial immune.